UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

U.S. SECURITIES AND EXCHANGE COMMISSION, )
)
Plaintiff, )
v. )
) Docket No. 21-CV-12088
VLADISLAV KLIUSHIN )
)
Defendant. )
)
)

**RESPONSE TO PLAINTIFF SEC'S MOTION FOR SUMMARY JUDGMENT**

Defendant Vladislav Kliushin, by and through undersigned counsel, hereby respectfully submits his response to the Securities and Exchange Commission's (hereinafter "SEC") Motion for Summary Judgment, Dkt. 49.

## I. Applicable Standard

In determining whether summary judgment is appropriate, "a court must view the record in the light most favorable to the nonmoving party and give that party the benefit of all reasonable inferences in its favor." *Clifford v. Barnhart*, 449 F.3d 276, 280 (1st Cir., 2006); *Guay v. Burack*, 677 F.3d 10, 13 (1st Cir., 2012). The burden is upon the moving party to show "that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed.R.Civ.P. 56(c). An issue is "genuine" if the evidence of record permits a rational factfinder to resolve it in favor of either party. *See Medina–Muñoz v. R.J. Reynolds Tobacco Co.*, 896 F.2d 5, 8 (1st Cir. 1990). A fact is "material" if its existence or nonexistence has the potential to change the outcome of the suit. *See Martínez v. Colón*, 54 F.3d 980, 984 (1st Cir. 1995).

## II. Argument

### A. Summary judgment should be denied based on the SEC's unprecedented theory of stock fraud.

This Honorable Court should deny the SEC's motion for summary judgment because its theory of stock fraud is unprecedented, never recognized by the First Circuit or the Supreme Court and attempts to expand federal securities laws to reach any act that touches upon a security – regardless of the whether there was a breach of a fiduciary duty or similar duty to disclose. This issue is presently pending before the First Circuit and Kliushin respectfully incorporates his appellate arguments herein. *See* Exhibit 1, Brief at 80-102.

The SEC's theory of liability in this case is not predicted upon any breach of duty. Indeed, its theory is that Kliushin, through Yermakov, using "various deceptive means to obtain material nonpublic pre-release earnings information of companies with shares of stock publicly traded on U.S. securities exchanges by gaining unauthorized access (i.e., hacking) into the computer systems of U.S.-based servicing firms." Dkt. 50 at 9. Entirely missing from the SEC's allegations is a breach of fiduciary duties owed to filing agents or to companies that they serviced. In essence, the SEC claims that any stolen information – even in the absence of fiduciary duties – is always actionable as securities fraud.

As relevant here, § 10(b) of the 1934 Securities Exchange Act "proscribes (1) using any deceptive device (2) in connection with the purchase or sale of securities, in contravention of rules prescribed by the [Securities and Exchange] Commission." *United States v. O'Hagan*, 521 U.S. 642, 651 (1997). Rule 10b-5, prescribed by the SEC in turn, outlaws, among other things, "mak[ing] untrue statements of material facts" or "omit[ting] to state material facts" in connection with "the purchase and sale of securities." 17 CFR § 240.10b-5

While intended to "insure honest securities markets and thereby promote investor confidence," *O'Hagan*, 521 U.S. at 658, these provisions are not "a broad federal remedy for all fraud," *Marine Bank v. Weaver*, 455 U.S. 551, 556 (1982), or a "blanket prohibition on illicit schemes that somehow involve securities transactions." *SEC v. Dorozhko*, 606 F. Supp. 2d 321, 324 (SDNY 2008) (*Dorozhko I*), *vacated*, 574 F.3d 42 (2d Cir. 2009) (*Dorozhko II*). They do "*not* reach all structural disparities in information that result in securities transactions," *id.*, and "must not be construed so broadly as to convert every common-law fraud that happens to involve securities into a [§ 10(b)] violation." In particular, the Supreme Court has long emphasized that a general "duty to disclose under § 10(b) does not arise from the mere possession of nonpublic market information," however acquired. *Chiarella v. United States*, 445 U.S. 222, 229, 235 (1980)

Over 90 years of interpretation since the Act's passage, the Court has "established that there are two complementary theories of insider trading liability" under § 10(b) and accompanying Rule 10b-5. Donna M. Nagy, *Insider Trading and the Gradual Demise of Fiduciary Principles*, 94 Iowa L. Rev. 1315, 1316 (May 2009) (Nagy). Under the "traditional" or "classical" theory, a "corporate insider" – permanent or temporary – "trades in the securities" of their corporation on the basis of "material, nonpublic information." *O'Hagan*, 521 U.S. at 651-52. Such trading counts as "deceptive" under § 10(b) because a "relationship of trust and confidence exists" between a corporation's shareholders and insiders who obtain "confidential information by reason of their [corporate] position." *Id.* at 652. And that relationship gives rise to a "duty to disclose" or "abstain from trading" so as to prevent corporate insiders from taking unfair advantage of uninformed stockholders – the counterparties to a purchase or sale. *Id.*; *see Chiarella*, 445 U.S. at 228 ("one who fails to disclose material information prior to the consummation of a transaction commits fraud only when … under a duty to" disclose).

Under the "misappropriation" theory, on the other hand, a malefactor "misappropriates confidential information for securities trading purposes, in breach of a duty owed to the [information's] source." *O'Hagan*, 521 U.S. at 652 On that theory, the Court elaborated, a fiduciary's

> undisclosed, self-serving use of a principal's information to purchase or sell securities, in breach of a duty of loyalty and confidentiality, defrauds the principal of the exclusive use of that information. In lieu of premising liability on a fiduciary relationship between company insider and purchaser or seller of the company's stock, the misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted him with access to confidential information.

*Id.*

At the heart or core of both established theories – insider trading's essential component and entire construct – is the requirement of a "fiduciary" relationship or similar duty of trust and confidence. *Dorozhko I*, 606 F. Supp. 2d at 338, 340-41; *SEC v. Rocklage*, 470 F.3d 1, 6 (1st Cir. 2006) ("when the trading individual owes no fiduciary duty to the stockholders of the traded-in corporation, and he has not obtained the information from one who has breached such a duty, there can be no insider trading liability under the classical theory"); *United States v. Kanodia*, 943 F.3d 499, 506 (1st Cir. 2019) ("Because the government prosecuted Kanodia on a misappropriation theory of insider trading, the jury needed to find that Kanodia breached a duty of trust and confidence owed to a corporate insider" who entrusted him with confidential information).

In sum, breach of a fiduciary or similar duty serves as the uniform "basis" or "predicate[]" for stock fraud liability under Supreme Court and First Circuit precedent; absent a fiduciary or similar breach, there is no deception within § 10(b)'s meaning and thus no insider trading violation. *Dorozhko I*, 606 F. Supp. 2d at 323-24, 330, 337-39. Stated simply, the high court has "explicit[ly] dictate[d] that fiduciary principles underlie the offense of insider trading" – of *any* stripe. Nagy, 94 Iowa L. Rev. at 1319; *id.* at 1323-24 & n.35 (calling fiduciary-like relationship "essential" to "either" recognized Supreme Court stock fraud theory (classical and misappropriation).

In the pending case, defendants are "true" corporate outsiders – not claimed to have "owed" or breached any fiduciary-type duty to either "market participants" or confidential information "source[s]." *Dorozhko I*, 606 F. Supp. 2d at 336. The SEC's allegations here is that Yermakov hacked into filing agent computers, extracted employee login credentials, and used them to steal material nonpublic information for trading by Kliushin and others. Courts and commentators have condemned this novel "hack-and-trade" theory as "greatly extend[ing] the reach of the SEC's policing power" and lacking "doctrinal foundation." Nagy, 94 Iowa L. Rev. at 1316. After all, § 10(b) "deception" is a term of art glossed by the Supreme Court over some 90 years, and it *consists of* – actually *resides in* – the existence and breach of a fiduciary-type duty. Accordingly, because Kliushin owed no such duty to any information source – either the filing agents or their corporate clients – or "to those he transacted with in the market," he could not have breached one "in connection with the purchase or sale of a security." *Dorozhko I*, 606 F. Supp. 2d at 324. It follows that the alleged "'hacking and trading' does not amount to a violation of § 10(b) and Rule 10b-5." *Id.*

As one judge, quoting a scholarly article, explained at some length:

> A … hacker who breaches the computer security walls of a large publicly held corporation and extracts nonpublic information may … trade and tip without running afoul of the insider trading rules. The … hacker may be liable for the conversion of nonpublic information under other laws, but the insider trading laws themselves appear not to prohibit the … hacker from trading or tipping on the basis of the stolen information. This is because there was no breach of a duty of loyalty to traders under the classic theory or to the source of the information under the misappropriation theory.

*Dorozhko I*, 606 F. Supp. 2d at 341-42.

By eliminating the crux of both § 10(b) deception and insider trading itself – the "requirement" of a fiduciary-type breach – the unorthodox "hack-and-trade" theory thus conflates theft and stock fraud, "undo[ing] decades of Supreme Court" and First Circuit "precedent" and "rewrit[ing] the law as it has developed. *Dorozhko I*, 606 F. Supp. 2d at 323, 340-41, 343.

Only one stray court swims against the prevailing academic and judicial tide. In *Dorozkho II*, a civil enforcement action, a panel of the Second Circuit Court of Appeals made the surprising and unprecedent assertion that Supreme Court securities precedent, closely read, strictly requires a fiduciary-type relationship only in cases involving omission or nondisclosure – and, concomitantly, that it does not foreclose § 10(b) liability without one in cases of affirmative misrepresentation. 574 F.3d 42. Twelve years later, in July 2021, a different panel of the same court summarily extended *Dorozkho II* to the criminal context in a single unreasoned sentence. *United States v. Khalupsky*, 5 F. 4th 279, 290 & n.30 (2d Cir. 2021). The Second Circuit's approach is severely flawed and should not prevail. *See Dorozkho II*, 574 F.3d at 45 (conceding that imposing § 10(b) liability "against defendant – a corporate outsider who owed no fiduciary duties to the source of the information – is not based on either of the two generally accepted theories of insider trading").

The *Dorozkho II* panel's analysis rests on a demonstrably faulty premise: that statutory interpretation begins by consulting applicable caselaw. 574 F.3d at 46 ("[i]n construing the text of any federal statute, we first consider the precedents that bind us as an intermediate appellate court"). In fact, as *Dorozkho I* properly recognized, the cardinal tenet of statutory interpretation is that construction both starts and ends – absent grievous ambiguity – with the text of the operative statute itself. 606 F. Supp. 2d at 327 ("As in all cases involving statutory interpretation, the appropriate starting point is the text of the statute itself.") (citing *Cent. Bank of Denver v. First*

*Interstate Bank of Denver*, 511 U.S. 164, 172-73 (1994), *superseded by statute on other grounds as stated in SEC v. Fehn*, 97 F.3d 1276, 1280 (CA9 1996))

The text of Rule 10b-5(b) juxtaposes and equates affirmative misrepresentations and material omissions or nondisclosures,[1] treating them as coterminous and qualitatively synonymous for purposes of securities fraud liability. Thus, far from supplying a textual basis to distinguish the two, the rule's plain language contradicts if not precludes any effort to do so. If omission liability requires a fiduciary-type breach, as even the *Dorozkho II* panel acknowledged, it follows that liability for affirmative misrepresentations does as well.

Language aside, settled law further belies the artificial distinction the *Dorozkho II* panel tried to draw. In *Santa Fe Indus. v. Green*, a 45-year-old case the panel conspicuously ignored, the Supreme Court pointedly "defined 'deception' as proscribed in § 10(b) as the making of a material misrepresentation *or* the non-disclosure of material information *in violation of a duty to disclose*."[2] *Dorozkho I*, 606 F. Supp. 2d at 330 (citing 430 U.S. 462, 470 (1977)) (emphasis supplied).

Beyond confounding law and language, any § 10(b) distinction between misrepresentations and omissions also defies simple common sense. Take the conduct alleged here. Remotely impersonating a filing agent employee – virtually passing yourself off as that individual – may be one man's affirmative misrepresentation but another's material omission – *i.e.*, failing to disclose the digital masquerade. They're two sides of the same functional coin. Similarly, while contending the former constitutes an affirmative misrepresentation and thus an actionable deception, the

[1] By its terms, Rule 10b-5(b) makes it "unlawful for any person, directly or indirectly," to "make any untrue statement of a material fact or to omit to state a material fact" in "connection with the purchase or sale of any security."

[2] *Dorozkho I*, 606 F. Supp. 2d at 330 (citing 430 U.S. 462, 470 (1977)) (emphasis supplied).

Second Circuit concedes uncertainty whether alternate, equally blameworthy forms of hacking – for example, using malware or SQL injection[3] to exploit a weakness in electronic code and gain unauthorized access – would qualify under its idiosyncratic rationale. *See Dorozhko II*, 574 F.3d at 50-51; *Khalupsky*, 5 F.4th at 291. A coherent, logical, administrable statutory scheme does not pin liability on arbitrary labels, semantic abstractions or the technical means a hacker happens to choose to infiltrate a protected computer.

This Honorable Court should reject the SEC's attempts to expand securities laws well beyond Supreme Court or First Circuit precedent. Furthermore, while Judge Saris denied Kliushin's motion to dismiss based on the same grounds in the criminal action. She called her decision a "“placeholder to see [how] the First Circuit" rules and ventured that it could "potentially … go a different way." *See* Exhibit 1, Brief at 82, n. 169. This Honorable Court is not bound by Judge Saris' decision and for the principled reasons above can and should decide otherwise.

### B. Summary judgment should be denied because there was no finding of venue pursuant to 15 U.S.C. §78aa or 15 U.S.C. §77v(a) and because no acts or transactions constituting the stock fraud occurred within this district.

The SEC cannot summarily preclude, based on collateral estoppel, Kliushin's venue defense because no jury found venue pursuant to 15 U.S.C. §78aa or 15 U.S.C. §77v(a). Moreover, the facts adduced at trial – the chance passage of information through a server in Boston, MA that neither Kliushin nor any conspirator knew about or undertook to use – cannot satisfy the relevant statutory venue provisions governing securities law claims. Dkt. 55 at 24-25. *See SST Glob. Tech., LLC v. Chapman*, 270 F. Supp. 2d 444, 452 (S.D.N.Y. 2003) ("Venue with regard to securities law

[3] According to the *Khalupsky* panel, SQL injection is a technique that enables intruders to "glean the architecture of [a] hacked computer system, identify vulnerabilities, and extract data." 5 F.4th at 291.

claims under the Securities Exchange Act is controlled exclusively by 15 U.S.C. § 78aa, without regard to the general venue provisions of 28 U.S.C. § 1391").

Despite objections from the defense, Judge Saris did not instruct on the specific venue provision relevant to substantive stock fraud, an issue currently under review by the First Circuit Court of Appeals. Exhibit 1, Brief at 78-79. At the government's request, the jury was instructed to evaluate stock fraud venue under 18 U.S.C. § 3237, the default statute for continuing offenses. *See id.*; *see also* Exhibit 1, Addendum at 49-51.[4] Consequently, no jury determined whether conduct implicating this district satisfies 15 U.S.C. §78aa, the broader of the two venue provisions, *i.e.*, no jury assessed whether "any act or transaction constituting the [stock fraud] violation occurred[]" in this district. *S.E.C. v. Spencer Pharm. Inc.*, 57 F. Supp. 3d 127, 137 (D. Mass. 2014) (internal quotations omitted).

Furthermore, the evidence adduced at trial regarding conduct that implicated this district, cannot as a matter of law, satisfy the requirements of 15 U.S.C. §78aa or 15 U.S.C. §77v(a). At trial, the only connection to this district was the chance passage of information packets through a third-party VPN server that – unbeknownst to Kliushin or any purported cohort – happened to be in Boston, MA. Indeed, there was no evidence that any relevant stock transaction occurred in this district or that any information was obtained from Massachusetts. Instead, the sole connection to this distrct was the location of a server that information passed through on its route between the computer belonging to the intruder (which, according to the government, was in Russia) and TM

[4] It was the government's position that an electronic signal passing through a district – even whereas here the electronic signals likely passed through nearly every district in the Unites States on their way from Russia and the filing agent servers in Illinois and Minnesota regardless of whether the transmission was intentional, knowing, or the product of an actual "act" by the defendant or a conspirator conferred venue in every passing district for a continuing offense under 18 U.S.C. § 3237. Exhibit 1, Brief at 47 and n.52.

and DFIN's servers (located respectively in Illinois and Minnesota).[5] *See* Exhibit 1, Brief at 30-47. The evidence was undisputed that the intrusions into the Illinois and Minnesota servers occurred over hundreds of IP addresses, belonging to regular internet providers and VPN providers, with servers all over the United States and internationally.[6] *See id.*, Brief at 8-10. Two of the hundreds of IP addresses appearing on DFIN's server logs between October 2018 and November 2018 (two months out of a purported years long scheme), were leased from Web2Objects by StackPath, a business-to-business and business-to-consumer VPN provider and assigned to its subsidiary Strong Technology LLC (Strong) as of May 18, 2018. *See id.*, Brief at 37. Neither Strong nor StackPath owned the servers that held the IP addresses. *See id.*, Brief at 37-38. Instead, they leased servers from Micfo, which purportedly placed the two IP addresses onto a server in Boston, MA.[7] There was no evidence that Kliushin, a conspirator, or anyone else had a choice to use the servers in Boston and no evidence Kliushin or anyone else could have known they were connected to the internet through a Boston server. *See* Exhibit 1, Brief at 39. Indeed, Strong did not advertise or provide a status for any Boston-based servers immediately before and

[5] During the Rule 29 hearing, the government argued that information was downloaded to the VPN server, but that argument was inconsistent with the testimony of its own witness and Strong's representations concerning how its servers function. *See* Exhibit 1, Brief at 40-41.

[6] According to Microsoft, a VPN – a "service" available on every internet enabled device anywhere in the world – "establishes a digital connection between your computer and a remote server owner owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address, and lets you sidestep website blocks and firewalls on the internet. This ensures that your online experiences are private, protected, and more secure." https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-isvpn (retrieved Mar. 4, 2023).

[7] Whether Micfo, a company that was convicted of fraud in the spring of 2019 in connection with fraudulent IP address practices, placed the servers in Boston was the subject of a factual dispute at trial. *See id.*, Brief at 38.

after the late October and early November intrusions. *See id.* In short, the use of an IP address ostensibly traced to Boston was strictly coincidental, predicated purely on chance. There was not a shred of proof that Kliushin or any coconspirator did anything – that they took any act – to route internet traffic through the Boston IP address.

"The Act meant to vest jurisdiction in every district where any use of such instrumentalities of the mail or interstate commerce ***was of material importance*** to the consummation of the scheme."[8] *Hooper v. Mountain States Sec. Corp.*, 282 F.2d 195, 205 (5th Cir. 1960); *SST Glob. Tech., LLC v. Chapman*, 270 F. Supp. 2d 444, 453 (S.D.N.Y. 2003) ("[t]he act or transaction committed within the district need not constitute the core of the violation, but should be an important step in the fraudulent scheme.") (internal citations and quotations omitted). Information passing through an IP address located in Bosotn – in contrast to any other IP address in the world – was simply not material to the alleged scheme. *See Ritter v. Zuspan*, 451 F. Supp. 926 (E.D. Mich. 1978) (sending a few documents to Michigan after execution of the agreement was not an act of material importance). The defense has not located a single case where venue was conferred simply because information, by chance, electronically flowed through a district without an "act" by the defendant. Generally, venue is proper in the originating or terminating locations of an electronic communication. *See e.g., Stern v. Gobeloff*, 332 F. Supp. 909, 911 (D. Md. 1971) ("[w]here an offer to sell securities is made by telephone by an offeror in one federal district and accepted by an offeree in another, part of the 'act or transaction constituting the violation' occurs in each district, and venue may be laid in either."). This makes sense given neither party have any control or knowledge over how a provider routes its calls. Similarly, no internet user knows or has

[8] 28 U.S.C. § 1391, the general venue statute, similarly provides that "[a] civil action may be brought in" "a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated."

control over how an internet provider routes its traffic. In short, the chance flow of information not caused by any act cannot, as a matter of law, confer venue. *See Pratt v. First California Co.*, 517 F.2d 11, 13 (10th Cir. 1975) ("unilateral" act of mailing certificates to Utah by plaintiff, who was not an agent or an aider or abettor of any defendant, did not confer venue – finding the mailing "a chance use of the mails" and that "no act or transaction of any defendant occurred in Utah");[9] *see also Travis v. United States*, 364 U.S. 631, 636 (1961). Otherwise, venue would be selected unilaterally and randomly by an internet service provider or telephone provider without regard to a defendant's actions or knowledge.

Because statutory stock fraud venue was never decided by the jury in the criminal case, summary judgment based on collateral estoppel should not be granted. Moreover, the defense respectfully submits that the facts adduced at the criminal trial cannot support venue in this district as a matter of law. The defense respectfully believes that at minimum this issue should be resolved by a jury, or alternatively, the case should either be transferred or dismissed.

### C. Summary judgment should be denied because the criminal case was submitted to the jury on a different theory of who was responsible for the hacking.

The SEC's complaint alleges that Defendant Yermakov "made material misstatements and used deceptive means, such as compromised employee credentials (*e.g.*, usernames and passwords that did not belong to him), malware, anonymized IP address, and other techniques, to gain unauthorized access to (*i.e.*, hacked into) the systems of two U.S.-based Servicers…" and that "Yermakov then, directly or indirectly, provided the hacked, deceptively obtained pre-release earnings announcements and/or access to those announcements through the Servicers' systems to Trader Defendants Kliushin, Rumiantcev, Irzak, and Sladkov, who are all Russian citizens and at

[9] There was no evidence that Stackpath or Strong were agents or aiders and abettors of Kliushin or a purported co-conspirator.

least during the Relevant Period resided in Russia." Dkt. 51 at 4-5; *see also* Dkt. 52-1 at 36-37 (charging Kliushin with adding and abetting Yermakov's violations). In essence, the SEC charged Yermakov with hacking and Kliushin with knowingly trading in hacked information. That, however, was not the only theory that the government argued to the jury in the criminal case.

Indeed, the evidence of Yermakov hacking the filing agents in the case was scant. During summation, the defense argued, in part, that the government's theory of Yermakov (also known as Ermakov) being the hacker that provided information to Kliushin and others was largely unsupported by the evidence:

> In its opening argument, the government promised to you to prove that Ermakov was the hacker. These are the words from just two weeks ago. There's no dispute that Ermakov worked for M-13. This is an employee list of all M-13 employees assigned to just one single project. It includes 46 people, nearly 20 engineers, 20 other professionals. There's no dispute that what's listed in this document is true. M-13 was a large company. It had many employees, both technical and administrative. They worked on large projects. There's no dispute that Ermakov was the Deputy Director General of M-13. There's no dispute that Mr. Rumiantcev was the Deputy Director. They were clearly part of the management team. But there's no evidence that Ermakov had the level of sophistication and computer wizardry necessary to pull off this complicated computer intrusion. If he was sophisticated, he would have been prominently featured amongst the various IT professionals that M-13 had at its employment.
>
> This is a proposal that Agent Hitchcock read a portion of. It's Exhibit 141. This is the last page. This is a proposal that Vlad submitted to a major company to provide penetration testing services. You can read it. It's 16 pages. It's detailed and extensive and includes all of the information about their services. The last page includes a list of experts that are assigned to the project. Ermakov is not the head of the Informational Security Department, or the head of the Penetration Testing Unit, or the head of the Security Analysis Unit, or the head of Audit and Consulting Unit. The only evidence that Ermakov is responsible for hacks is in one IP address that overlaps with DFIN logs and was located on his iTunes application.
>
> This is the log file showing that the IP address in May 9th of 2018 was used by Mr. Ermakov to update his Mac apps. We know from Mr. Roberts' testimony that there's simply not enough IPs in the world to accommodate every person, every business, every internet-connected device. We have to share them with our neighbors, with our friends, with strangers, and everybody else. He testified there could be thousands, tens of thousands, hundreds of thousands of people using the

> same IP address every day. You and I likely have the same IP address. It's not strange. It's just the way the Internet works.
>
> So what do we know about this IP address specifically? Nothing. You didn't receive any information about it. You have not heard any testimony about who it belongs to, who serviced it, or whether it was associated with any VPN. You know it was an AirVPN address; it was not a StackPath address. The evidence relating to this IP address is just absent. Why didn't the government present any evidence about the IP? I don't know. Ask yourself, though, was it likely that this IP was shared by hundreds of thousands of people at the same time? And based on Mr. Roberts' testimony, I believe it's an affirmative "yes."
>
> There's another hole in the evidence that I don't understand and I can't even begin to explain to you. We all know that iTunes means you have a Mac. You can't update an Android or a Windows from the Apple iTunes store. It's common knowledge. It makes perfect sense. You're talking about two completely different programming ecosystems. Just like an iPhone user doesn't update their phone from a Google Playstore, PC users don't update their applications from iTunes.
>
> Mr. Brawner from Kroll and Mr. Hartvigsen from StoneTurn, whose twelve-person team investigated the intrusions at DFIN, they both told you that the intrusions took place using a Windows computer. The computer intruding and Ermakov's Mac are completely two different computers. There's no evidence that Ermakov ever used a Windows laptop. The only people in this case that used a Windows computer are people who took selfies of themselves with earnings reports on their Windows laptop, Mr. Sladkov and Mr. Irzak.
>
> If there's a person that the government wants to point the finger at as the hacker, as the perpetrator, they shouldn't point the finger at Ermakov or Vlad. They should point the finger at Sladkov. He's the only person in this case to use a PC, the only person to have an earnings report prior to its release, not on one occasion, not on two occasions, but on three occasions. He's the only person to have a trading account in 2017, which is the start of the intrusions. This is reasonable doubt about the government's theory. Their theory is dependent on Ermakov being the hacker because he is close to Vlad, but the evidence doesn't support it.
>
> ***

Dkt. 52-9 at 65-69.

In response, the government pivoted its theories to include Sladkov as the hacker who passed information to Yermakov and others. *See* Exhibit 2 ("And PS, there can be more than one hacker involved. It doesn't have to be only Ivan Ermakov. It wasn't only Ivan Ermakov. He was the defendant's close buddy. He was the hacker involved in this scheme. So was Igor Sladkov…”). Given the general jury verdict, it’s unclear which theory the jury adopted in finding Kliushin guilty. In essence, the verdict in the criminal case could have been based on a factual theory different than the one charged by the SEC. For these reasons, summary judgment is inappropriate under the circumstances, and certainly inappropriate, under an aiding and abetting theory.

## III. Conclusion

For all the foregoing reasons, this Honorable Court should deny the SEC’s Motion for Summary Judgment.

Respectfully Submitted,

Vladislav Kliushin,
By His Attorney,

**/s/ Maksim Nemtsev**
Maksim Nemtsev, Esq.
Mass. Bar No. 690826
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700
menemtsev@gmail.com

Dated: April 12, 2024

## CERTIFICATE OF SERVICE

I, Maksim Nemtsev, hereby certify that on this date, April 12, 2024, a copy of the foregoing documents has been served via Electronic Court Filing system on all registered participants.

**/s/ Maksim Nemtsev**
Maksim Nemtsev